Huntington Hospital
Northwell Health
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 24, 2021

H1048-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 PATIENT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Dear Sample A. Sample:

The purpose of this letter is to notify you about an incident at Huntington Hospital ("we" or "us") that involved your health information.

What Happened?

On February 25, 2019, we determined that an employee at Huntington Hospital improperly accessed certain electronic medical records without role-based authorization between October 2018 and February 2019. Your medical record from [Current_Location] was among the impacted records. Once we became aware of the employee's conduct, we immediately began a thorough investigation and deactivated his access to our electronic medical record systems. The employee was subsequently terminated. In addition, we reported the matter to law enforcement. Huntington Hospital cooperated fully with the law enforcement investigation, which included following law enforcement's instructions to delay notifying any patients who were potentially impacted by this incident through November 2021. The law enforcement investigation resulted in the former employee being charged with a criminal HIPAA violation by the federal government.

What Information Was Involved?

There is no evidence that your Social Security number, insurance information, credit card number or any other payment-related information were accessed. Categories of personal information varied for each affected patient and may have included the following: (1) demographic-type information such as your name, date of birth, telephone number, address, internal account number and medical record number; and (2) clinical information such as diagnoses, medications, laboratory results, course of treatment, the names of health care providers, and/or other treatment-related information.

What We Are Doing.

Please know that Huntington Hospital has taken numerous steps to protect the confidentiality of your information and to prevent this type of incident from occurring in the future. These actions include terminating the employee involved in the unauthorized access of personal information and implementing additional security tools to monitor access to our medical record applications. Moreover, we provided employee training and targeted re-training of front-line staff on the importance of protecting patient confidentiality and safeguarding health information. Finally, the Office of Corporate Compliance conducts audits of medical record access to minimize the risk of such incidents occurring in the future, and as a result of this incident, we have reviewed and revised our policies and procedures governing those audits.

As an added precaution, we are offering a complimentary one-year membership of Experian IdentityWorks[SM] to protect your identity. Please note that Identity Restoration is available to you for **one year** from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

What You Can Do.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks[SM] as a complimentary **one-year** membership. This product provides you with superior identity detection and resolution of identity theft.

You will find detailed instructions for enrollment on the enclosed Additional Details document. Moreover, the enclosed Recommended Steps document provides further information about steps that you can take. In addition to the steps we have taken, we encourage you to regularly review your financial accounts and report any suspicious or unrecognized activity immediately.

Other Important Information.

The privacy and security of your personal information is a very serious matter for us. We regret this occurrence and apologize for any inconvenience or concern that it may cause you. It is our intention, through the quality and reliability of the services we are offering to you, to demonstrate our continued commitment to your security and satisfaction. Should you have any questions or concerns regarding this matter, please do not hesitate to contact us at (833) 671-0408.

Sincerely,

Janice Stewart
Assistant Vice President
Corporate Compliance

Enclosures

Additional Details Regarding Your One Year Experian IdentityWorks℠ Membership

To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by February 24, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks℠ website to enroll: **https://www.experianidworks.com/RR1Bplus**
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 671-0408** by **February 24, 2022**. Be prepared to provide engagement number B021558 as proof of eligibility for the Identity Restoration services by Experian.

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only*.
- **Credit Monitoring:** Actively monitors your Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet**: Provides assistance with canceling/replacing lost or stolen credit, debit, and medical cards.
- **Child Monitoring**: For 10 children up to 18 years old, Internet Surveillance and monitoring to determine whether enrolled minors in your household have an Experian credit report are available. Also included are Identity Restoration and up to $1M Identity Theft Insurance.

*Offline members will be eligible to call for additional reports quarterly after enrolling.

**The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to Experian's customer care team. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration specialist is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity).

Recommended Steps You Can Take to Protect Your Personal Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

State Specific Information

New York residents can learn more about security breach response and identity theft prevention and protection information by visiting the New York Attorney General Office's website at https://ag.ny.gov, or calling 1-800-771-7755, or visiting the New York Department of State Division of Consumer Protection website at http://www.dos.ny.gov/consumerprotection or calling 518-474-8583 / 1-800-697-1220.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their website https://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 1-919-716-6400 or 1-877-566-7226, or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.